

DERWENT-ACC-NO: 1988-230777

DERWENT-WEEK: 198833

COPYRIGHT 2005 DERWENT INFORMATION LTD

TITLE: IC card for cash or credit card - has
microprocessor and data memory with publisher key storing region
and verification region. NoAbstract Dwg 0/5

PATENT-ASSIGNEE: MATSUSHITA ELEC IND CO LTD [MATU]

PRIORITY-DATA: 1986JP-0312054 (December 26, 1986)

PATENT-FAMILY:

PUB-NO	PUB-DATE	LANGUAGE
PAGES MAIN-IPC		
JP 63163690 A	July 7, 1988	N/A
006 N/A		

APPLICATION-DATA:

PUB-NO	APPL-DESCRIPTOR	APPL-NO
APPL-DATE		
JP 63163690A	N/A	1986JP-0312054
December 26, 1986		

INT-CL (IPC): B42D015/02, G06K019/00, H01L027/10

ABSTRACTED-PUB-NO:

EQUIVALENT-ABSTRACTS:

TITLE-TERMS: IC CARD CASH CREDIT CARD MICROPROCESSOR DATA MEMORY KEY
STORAGE

REGION VERIFICATION REGION NOABSTRACT

DERWENT-CLASS: P76 T01 T04 U13

EPI-CODES: T01-H01B; T01-H01C; T04-K; U13-C04B; U13-C05;

⑫ 公開特許公報 (A) 昭63-163690

⑬ Int.Cl. ¹	識別記号	庁内整理番号	⑭ 公開 昭和63年(1988)7月7日
G 06 K 19/00		Q-6711-5B	
B 42 D 15/02	331	J-8302-2C	
G 06 K 19/00		P-6711-5B	
H 01 L 27/10	461	8624-5F	審査請求 未請求 発明の数 1 (全4頁)

⑮ 発明の名称 ICカード

⑯ 特願 昭61-312054

⑰ 出願 昭61(1986)12月26日

⑮ 発明者 高木 伸哉	大阪府門真市大字門真1006番地	松下電器産業株式会社内
⑯ 発明者 飯山 恵市	大阪府門真市大字門真1006番地	松下電器産業株式会社内
⑰ 発明者 藤本 和生	大阪府門真市大字門真1006番地	松下電器産業株式会社内
⑱ 出願人 松下電器産業株式会社	大阪府門真市大字門真1006番地	
⑲ 代理人 弁理士 中尾 敏男	外1名	

明細書

1. 発明の名称

ICカード

2. 特許請求の範囲

マイクロプロセッサとデータメモリを具備し、前記データメモリが、発行者キーを格納するための発行者キー格納領域と、データの読み出し及び書き込みを実行するに先立ち前記発行者キーの照合を必要とする機密領域と、購入価格格納領域とを有し、前記購入価格格納領域は、金額の減少が前記発行者キーの照合後のみ行なえ、金額の読み出し及び金額の増加が前記発行者キーの照合を必要とせずに行なえる構成としたICカード。

3. 発明の詳細な説明

産業上の利用分野

本発明はキャッシュカード、クレジットカードなどに用いられるICカードに関するものである。

従来の技術

従来のICカードのメモリフォーマットは、例えば第4図に示すような構成であった。第4図に

おいて、40は発行者キーを格納するための発行者キー格納領域、41は発行者キーの照合が正常に行なわれた後にアクセスが可能となる機密領域である。従来のICカードを端末からアクセスする手順を第5図に示し、以下その動作を説明する。まず、初めに端末はICカードに対してリセット信号を出力し、ICカードを初期化する。初期化処理を終了したICカードは、リセット信号に対する応答としてカードの識別情報(アンサ・トゥ・リセット)を返送する。次に端末はICカードをアクセスする権利を得るため、ICカードに対して発行者キーを送信する。ICカードは受信した発行者キーと、発行者キー格納領域40に格納されているデータとを照合して、一致したか否かの情報を端末に返送する。照合が一致した場合、それ以降端末はICカード内の機密領域41に対して自由にアクセスが可能となる。一方、照合が一致しなかった場合はICカード内の機密領域41に対して一切アクセスすることが出来ない。このように発行者キーの照合が正常に行なわれない限

り、ICカード内の全ての情報を読み書き出来ない構成となっていた。

発明が解決しようとする問題点

このような従来のICカードを使用するために、全ての端末が発行者キーを保有している必要がある。一方、発行者キーはICカードが不正使用されないための極めて重要な機密データであり、様々な場所に設置される端末に、この発行者キーを保有させるようなことは保安上好ましくない。したがって各個人は限られた端末でしかICカードを利用することが出来ず、このことがICカードの用途を制限していた。本発明はこのような問題を解決するもので、発行者キーを保有していない端末でも読み書きが出来るICカードを提供することを目的とするものである。

問題点を解決するための手段

この問題点を解決するために本発明は、ICカード内のデータメモリが、発行者キーを格納するための発行者キー格納領域と、データの読み出し及び書き込みを実行するに先立ち前記発行者キー

金額〇を書き込む。この操作は購入価格格納領域12のデータの値を減らして書き換える操作であるため、発行者キーを保有している発行主体（銀行）の端末でのみ実行可能である。そしてICカード保有者がICカードを用いて買い物をする度に、購入価格が購入価格格納領域12に加算される。この作業は購入価格格納領域12のデータの値を増やして書き換える操作であるため、発行者キーの照合を必要としない。したがって販売店に設置されている端末が発行者キーを保有している必要はない。購入価格格納領域12のデータは、発行者キーの照合が正常に行なわれない限り、値を減らして書き換えることが出来ないため、勝手に金額を減らす等の不正使用をされることはない。

以上の使用において、発行主体は従来と同様第5図の手順により機密領域11をアクセス出来る。またクレジット会社は上述した購入価格格納領域12のみのアクセスが可能であるが、それは第3図に示す手順で行なわれる。すなわち、この時は第5図に示す手順とは異なり、発行者キーの照合

の照合を必要とする機密領域と、購入価格格納領域とを有し、前記購入価格格納領域は、金額の減少が前記発行者キーの照合後ののみ行なえ、金額の読み出し及び金額の増加が前記発行者キーの照合を必要とせずに行なえる構成としたものである。

作用

この構成により、端末機が発行者キーを保有することなく、購入価格をアクセス出来るため、例えばクレジットカードとしてもICカードを利用することが出来ることとなる。

実施例

第1図は本発明の一実施例によるICカードのメモリフォーマットであり、第1図において10は発行者キー格納領域、11は機密領域、12は購入価格格納領域である。以上のようなメモリフォーマットを持つ本実施例におけるICカードの利用例について以下説明を行なう。発行主体（銀行）は、発行者キーを保有する端末を用いて、発行主体以外が利用してはいけない情報を機密領域11に書き込み、さらに購入価格格納領域12に

を行なうことなく、直ちに各処理に行けるのである。

次に、本発明の他の実施例について図面を参照しながら説明する。第2図は、本発明の他の実施例におけるICカードのメモリフォーマットを示すものである。第2図において、20は発行者キー格納領域、21はPIN（個人暗証番号）格納領域、22は機密領域、23はPIN必須指定フラグ、24は購入価格格納領域である。銀行のATMやCDを使用する場合は、常に本人が正しいPINを入力する必要があるが、クレジットで買い物をする時のように大金を扱わない場合は、PINの入力を必要とするか否かを個人が選択できるようにしておくことが望ましい。PIN必須指定フラグ23は前記目的のため使用されるもので、当フラグ23がオフにセットされている場合は、購入価格格納領域24をアクセスする際に、PIN照合を必要としない（即ち、クレジットで買い物をする際に、PINの入力を必要としない）ことを指定している。ただしこの場合は、購入価

格納領域に書き込める金額の最大値を設定できるようにしておくことが望ましい。

発明の効果

以上のように本発明によれば、ICカード内のデータメモリが発行者キーを格納するための発行者キー格納領域と、データの読み出し及び書き込みを実行するに先立ち発行者キーの照合を必要とする機密領域と、購入価格格納領域とを有し、前記購入価格格納領域は、金額の減少が前記発行者キーの照合後ののみ行なえ、金額の読み出し及び金額の増加が前記発行者キーの照合を必要とせずに行なえる構成とすることにより、セキュリティを低下させることなく、例えばクレジットカードとしても使用出来るICカードを提供出来ることとなり、ICカードの利用範囲を大きく拡大するものである。

4、図面の簡単な説明

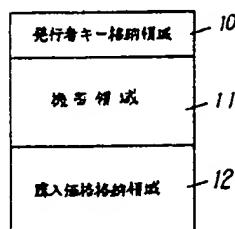
第1図は本発明の一実施例によるICカードのメモリフォーマットを示す図、第2図は他の実施例によるICカードのメモリフォーマットを示す

図、第3図は例えばクレジットで本発明のICカードをアクセスする場合のアルゴリズムを記述したフローチャート、第4図は従来のICカードのメモリフォーマットを示す図、第5図は端末が従来のICカードをアクセスする場合のアルゴリズムを記述したフローチャートである。

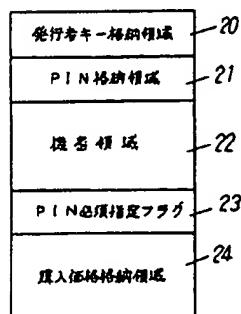
10, 20, 40 …… 発行者キー格納領域、
11, 22, 41 …… 機密領域、12, 24 ……
購入価格格納領域、21 …… PIN格納領域、
23 …… PIN必須指定フラグ。

代理人の氏名 弁理士 中尾 敏男ほか1名

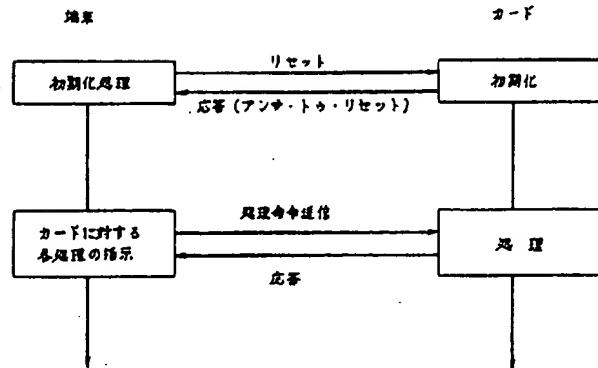
第1図



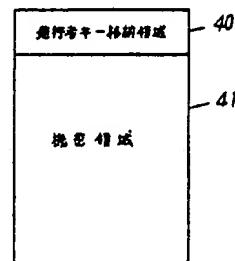
第2図



第3図



第4図



第5図 基本

